ENC. 3

**KPMG LLP**
Suite 2000
355 South Grand Avenue
Los Angeles, CA 90071-1568

November 14, 2007

The Board of Water and Power Commissioners
Department of Water and Power
City of Los Angeles, California

Ladies and Gentlemen:

We have audited the financial statements of the Power Revenue Fund (Power System) and the Water Revenue Fund (Water System), enterprise funds of the City of Los Angeles, California (collectively referred to as the Department) for the year ended June 30, 2007, and have issued our reports thereon dated November 14, 2007. In planning and performing our audit of the financial statements of the Department, in accordance with auditing standards generally accepted in the United States of America, we considered the Department's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements but not for the purpose of expressing an opinion on the effectiveness of the Department's internal control. Accordingly, we do not express an opinion on the effectiveness of the Department's internal control.

During our audit, we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized in the following pages.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements and, therefore, may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the department's organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

This communication is intended solely for the information and use of the audit committee, management, and others within the organization and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

6/23/08
Mgt Ltr

**1. Lack of Signed Information Technology Services Security Agreement Form**

***Observation***

Based on our testwork, we noted one user that had no Information Technology Services Security Agreement form on file. In addition, we noted that two employees did not have a signed form on file.

***Recommendation***

We recommend that management recommunicate the formal policy and procedures over the proper completion of the LADWP Information Technology Services Information Security Agreement Form to all appropriate personnel. This form is required to be completed for all new users of any LADWP IT application.

***Management Response***

The Security Agreement policy and procedure is being revised so that all employees and consultants must sign an LADWP Information Technology Services Information Security Agreement Form annually.

The Information Security Manager is in the process of revising the LADWP Information Technology Services Information Security Agreement Form and updating the policy (in collaboration with Enterprise IT Security Section) and procedures.

**2. Weak Logical Access Controls**

***Observation***

Based on our testwork, we noted that password configuration for the various applications (Accounts Payable System (APS), Employee Information System (EIS), Walker/General Ledger (GL), Human Resources Management System (HRMS) and Responsibility Cost Accounting System (RCAS) did not adhere to leading password standards. We identified the following issues regarding proper operations and configurations for application password parameters:

(1) We noted that the APS does not have a separate authentication apart from the mainframe. User access is controlled by the specific designated APS groups.

(2) We noted that to gain access to EIS the user must first be granted access to the Mainframe, which is controlled by RACF security. The user then must sign on separately to EIS. We noted that the system requires that passwords have a minimum of five characters. Due to system limitations, EIS cannot perform more password constraints, to adhere to leading practice password standards.

(3) We noted that to gain access to the GL, the user must first be granted access to the Mainframe, which is controlled by RACF security. The user then must sign on separately to the GL. We noted that the system requires that passwords have a minimum of one character. Due to system limitations, GL cannot perform more password constraints, to adhere to leading practice password standards.

(4) We noted that RCAS requires passwords to have a minimum of five characters and a maximum of eight characters. In addition, we noted that due to system limitations, RCAS cannot perform more password constraints, to adhere to leading password standards.

(5) We noted that the PeopleSoft HRMS application requires passwords to have a minimum of three characters. PeopleSoft HRMS v7.5 does not provide the functionality to support leading practice passwords. In addition, Peoplesoft system is not configured to prompt the user to change the password upon first log on.

***Recommendation***

We recommend that management incorporate stricter password restrictions on the key financial applications (APS, EIS, Walker/GL, HRMS, and RCAS). User access control in the Department's critical systems should be strengthened to guard against inappropriate access. A password policy should indicate that all platforms and systems should adopt the password usage where applicable. Below are the recommended password guidelines:

Minimum password length: 6 – 8
Change at first login: Yes
Password Change interval: 30 – 90 days
Concurrent Sessions: 1
Invalid log-on attempts: 3 – 5
Lockout period: Admin Reinstate or 24 hours
Password History: 5 – 8

***Management Response***

In addition to the current internal application security, IMS RACF transaction security is in the process of being implemented for APS, EIS, RCAS, and Walker/GL applications. The Information Security Manager will supply a list of IMS transaction names, grouped by functional roles and users who are authorized to run those transactions, which will be secured by the IT RACF Security Administrator.

The HRMS PeopleSoft is running unsupported version 7.5. The Information Security Manager is in the process completing an investigation on how to implement stronger password and access controls on this version of PeopleSoft.

The current password policy and guidelines for RACF and Joint and Power Active Directory meet or exceed the majority of the recommended guidelines. The Water Active Directory policy settings is in the process of being changed to match the Joint and Power AD settings. The current policy settings are noted below:

| Minimum password length | RACF | AD Joint/ power | AD Water | DWP Proposed policy |
|---|---|---|---|---|
| Minimum password length | 7 | 7 | 7 | 7 |
| Change at first login | Yes | Yes | Yes | Yes |
| Password change interval | 90 days | 90 days | Never | 90 days |
| Concurrent sessions | Multiple IMS | 1 | 1 | 1 |
| Invalid log-on attempts | 3 | 6 | — | 6 |
| Lockout period | Admin Reinstate | Admin Reinstate | Admin Reinstate | Admin Reinstate |
| Password history | 10 | 10 | 10 | 10 |

A more complete Identity Management solution providing access management and provisioning solution is currently being investigated. The projected schedule for the project is as follows:

| | |
|---|---|
| Project Start | May 2008 |
| Web Access | July 2008 |
| Central repository | Nov 2008 |
| Initial Provisioning | Feb 2009 |
| Auditing | July 2009 |

**3. Weak Access to Security Administrator Account**

***Observation***

Based on our testwork, we noted that the security administrator account (99RCA) is a single administrator account that cannot be assigned to individual users. The password is shared.

***Recommendation***

We recommend that the Department document all system accounts and the controls in place to ensure that only appropriate users access them. This may include controls such as ensuring that the user ID is defined as system ID (no password and only accessible by application programs), ensuring that password is not trivial, keeping the ID locked until the vendor/contractor requires its use, monitoring it to ensure that it has not been used and/or when it is in use, etc.

Authorized administrators should be administering the system with unique individual user IDs rather than generic system accounts. We recommend that all accounts have an owner associated with them and each user only have one account. As noted above, this includes documenting the controls in place to ensure that appropriate users access the vendor or system IDs.

We recommend that management carefully identify and review all users that require 'administrator' privileges to the systems/applications. An assessment should be made to determine which IT

personnel require privileged access to perform their daily job responsibilities. For each appropriate 'administrative' user, a unique ID should be created and they should be required to only utilize their own ID to perform 'administrative' responsibilities.

***Management Response***

The Information Security Manager will document all system accounts and the controls in place to verify that only appropriate users have access to them. The Information Security Manager will develop a policy (in collaboration with Enterprise IT Security Section) and procedure that require a periodic review of all admin accounts. These tasks are in progress.

Additionally an audit of all privileged accounts is in the process of being completed to ensure that privileged access is limited to those whose job functions require it and that there is adequate segregation of duties.

IMS RACF transaction security will be implemented to restrict access to RCAS admin transactions to users identified as requiring privileged accounts. The RACF security will be in addition to the current application based security. The Information Security Manager will supply a list of RCAS admin IMS transaction names and users who are authorized to run those transactions. These transactions will be secured by the IT RACF Security Administrator.

The identity management initiative will improve access controls by breaking system accounts and providing individual administrative accounts. As part of the identity management project, each application privileged accounts will be audited. Policies for granting, reviewing, and revoking access will be put in place.

A more complete Identity Management solution providing access management and provisioning solution is currently being investigated. The projected schedule for the project is as follows:

| | |
|---|---|
| Project Start | May 2008 |
| Web Access | July 2008 |
| Central repository | Nov 2008 |
| Initial Provisioning | Feb 2009 |
| Auditing | July 2009 |

**4. Weak "VIP" Access Controls for Employee Information System (EIS)**

***Observation***

Based on our testwork, we noted that the system administrator access to grant batch numbers to user ID's is available to anyone with the "VIP" access in EIS. Per inquiry of Payroll & Timekeeping Assistant Chief Timekeeper, VIP access is a common level of access within the Timekeeping module. The access in Payroll is considered "All or Nothing" and several people have access. She informed us that only three (3) people know the menu path for granting batch numbers. We noted that although the menu path is extensive (Timekeeping, Main Timekeeping, Parameter Tables, and Miscellaneous Code), there is, currently, no way of restricting access. We noted that although users can access this menu, they are still required to know the specific codes to assign batch numbers.

***Recommendation***

We recommend that management consider modifying access controls within the EIS application in order to appropriately segregate access to grant batch numbers to restricted personnel. Specific access, such as granting batch numbers, should be segregated from the standard update privilege given to all payroll personnel. Management should carefully identify and review all users that require access to granting batch numbers and ensure that access is appropriately restricted to these individuals.

***Management Response***

The Information Security Manager is in the process of documenting all EIS accounts and the controls in place to verify that only appropriate users access them. The Information Security Manager is currently developing a policy (in collaboration with Enterprise IT Security Section) and procedures that require periodic review of all admin accounts.

ITSD is in the process of completing an audit of users having privileged access to EIS. Access to the program that allows batch numbers to be assigned will be restricted via RACF. Access will be restricted to only a subset of the "VIP" users whose responsibilities require that level of access.

IMS RACF transaction security will be implemented to restrict access to EIS admin transactions, which will be in addition to the current application based security. The Information Security Manager will supply a list of EIS admin IMS transaction names and users who are authorized to run those transactions, which will be secured by the IT RACF Security Administrator.

**5. Inappropriate Access to Operations Room (Data Center)**

***Observation***

Based on our testwork, we noted that 3 of 145 employees were granted inappropriate access to the Operations Room 214. The employees did not require physical access to the operations room (data center) as part of their job responsibility.

***Recommendation***

We recommend that management review the system generated listing of users with access to the Data Center to ensure that only appropriate personnel, with the daily job responsibilities which require access, continue to have access to the Data Center.

On an ongoing basis, we recommend that management develop and implement a formal procedure over the granting and removing of access to the Data Center. Specifically:

- A formal User Request Form should be completed, with approvals, for all data center access requests.
- The confirmation of the user being granted access should be evidenced.

The request and approval evidence should be documented and formally evidenced. A process, which evidences the proper approvals required by management, will ensure that all users with access are

approved and authorized to have direct access to the server room where the financial applications are maintained.

***Management Response***

A review of the system generated listing of users with access to the Data Center is conducted monthly. The last review was completed by Data Center Management in April 2008.

The Information Security Manager will develop a formal policy (in collaboration with Enterprise IT Security Section) and procedure that will require use the ITSR system to request changes to Data Center access privileges. A new category type will be created to track this type of requests.

**6. Inappropriate Mainframe and Network Access**

***Observation***

Based on our testwork, we noted that 13 out of 15 users have mainframe and network access. With the assistance of the Data Security Administrator and through inspection of Information Technology Services Request (ITSR) forms for selection, we noted that these access were not approved. Hence, we were unable to determine whether these users were appropriately authorized.

***Recommendation***

We recommend that management develop and implement a formal procedure over granting of access and setup of new users. Specifically:

- A formal User Request Form should be completed and approved, for all new users.
- Department Leads should determine the access rights of the new user and evidence their approval on the User Request Form.
- The confirmation of the user account being created should be properly evidenced.

The request and approval evidence should be documented and formally evidenced. This procedure should also cover the requesting of new user access as well as requesting access changes to current users.

Over time, changes in personnel, job positions, system environments, and business practices may cause user access to become inappropriate. Also, the turnover of personnel will result in the required removal of user access. Management should establish formal procedures over the disabling and/or the complete removal of terminated users from the critical systems/applications. In the event that a user is required to be 'disabled' only, a specified approval should be captured as well as determining a specific length of time the 'disabled' ID will remain on the system/application.

***Management Response***

A formal request form is currently in place as part of the ITSR system. The ITSR system requires appropriate approvals prior to granting access.

The Enterprise IT Security Policy, which is currently being drafted, addresses removal of access from employees and contractors who no longer work for LADWP, and access changes for employees

and contractors whose work role has changed requiring different access rights. Initially, this will be based on a payroll report sent bimonthly to IT RACF and AD Security Administrators. The IT RACF and AD Security Administrators will update AD and RACF to reflect the changes.

The Information Security Manager will develop formal procedures requiring access be removed from employees and contractors who no longer work for LADWP, and changed for employees and contractors whose work role has changed requiring different access rights.

A more complete Identity Management solution providing access management and provisioning solution is currently being investigated. The projected schedule for the project is as follows:

| | |
|---|---|
| Project Start | May 2008 |
| Web Access | July 2008 |
| Central repository | Nov 2008 |
| Initial Provisioning | Feb 2009 |

**7. Inconsistent and Informal Review Process for Accounts Payable System (APS) Access**

***Observation***

Based on our testwork, we noted that to obtain and/or update access to APS, which includes the creation of vouchers, a user must be 'connected' to the RACF 'AP Group' security group. To request access to the 'AP Group,' a user either includes the request during the ITSR mainframe request process or e-mails/calls the Data Security Administrator, who then calls a Senior Clerk for verification and approval. Once verified for approval, the Data Security Administrator sets up the user. We noted that this process is currently inconsistent, informal, and may not be documented.

***Recommendation***

We recommend that management develop and implement a formal procedure over the granting of access and setup of new users. Specifically:

- A formal User Request Form should be completed and approved, for all new users.
- Department Leads should determine the access rights of the new user and evidence their approval on the User Request Form.
- The confirmation of the user account being created should be properly evidenced.

The request and approval evidence should be documented and formally evidenced. This procedure should also cover the requesting of new user access as well as requesting access changes to current users.

Over time, changes in personnel, job positions, system environments, and business practices may cause user access to become inappropriate. Also, the turnover of personnel will result in the required removal of user access. Management should establish formal procedures over the disabling and/or the complete removal of terminated users from the critical systems/applications. In the event that a user is required to be 'disabled' only, a specified approval should be captured as well as determining a specific length of time the 'disabled' ID will remain on the system/application.

***Management Response***

For APS, a formal request form is currently in place as part of the ITSR system. The ITSR system requires appropriate approvals prior to access being granted.

The Enterprise IT Security Policy, which is currently being drafted addresses removal of access from employees and contractors who no longer work for LADWP, and access changes for employees and contractors whose work role has changed requiring different access rights. Initially, this will be based on a payroll report sent bimonthly to IT RACF and AD Security Administrators. The IT RACF and AD Security Administrators will update AD and RACF to reflect these changes.

A more complete Identity Management solution providing access management and provisioning solution is currently being investigated. The projected schedule for the project is as follows:

| | |
|---|---|
| Project Start | May 2008 |
| Web Access | July 2008 |
| Central repository | Nov 2008 |
| Initial Provisioning | Feb 2009 |

**8. Periodic Review of User Access Rights**

***Observation***

Based on our testwork, we noted there is no review of user access rights performed by the Department. In addition, there is no review over segregation of duties to ensure that access to key application role profiles or role-based access is appropriate.

***Recommendation***

We recommend that management implement processes and procedures for conducting user access reviews. These reviews should be performed in collaboration with business units and the IT department since the business unit has knowledge on the processes and business rules of their department. Evidence of such reviews should be logged and kept. A detailed review should be performed over the validity of all users and their access to the critical systems. This review should be conducted to ensure that only active employees have access to the network, and appropriate users have access to the critical systems and their access is aligned with their job responsibilities. Based on the results of the review, management should undertake appropriate steps to make necessary adjustments to user access to the critical systems.

We recommend that management create a role-based security access matrix, which should list, at a minimum, the transactions that should not be grouped together and profiles that should not be assigned together that would result in a segregation of duties conflict. Careful consideration should be taken into account for roles or profiles that are determined to be a conflict to ensure that a segregation of conflict is maintained. This matrix should be reviewed during the maintenance/creation of profiles and during the assignment of user access.

In addition, user access should be reviewed against the access matrix to ensure that user access is in compliance with the Department's segregation of duties policies. Compensating controls should be required in situations where users may have segregation of duties conflicts. Based on the results of

the review, management should undertake appropriate steps to make necessary adjustments to user access to the critical systems.

***Management Response***

The Information Security Manager is in the process of developing a policy (in collaboration with Enterprise IT Security Section) and procedures to perform Periodic Review of User Access Rights.

The Information Security Manager will collaborate with Business Users to develop a role based security access matrix, which will address segregation of duty conflicts. This matrix will be used to develop and implement IMS RACF security groups to protect sensitive transactions.

**9. Retention of Security Violation Reports**

***Observation***

Based on our testwork, we noted that the mainframe system provides security violation reports that identify users who have unsuccessfully accessed a particular file or users who attempted certain transactions. Based on a walkthrough of the monitoring of these reports, we noted that the Data Security Administrator reviews and monitors the mainframe security violation reports online daily and e-mails users who have unsuccessfully accessed a particular file or attempted a certain transaction to determine the reason behind the activity. We noted that these reports are not retained and that the follow-up emails are not retained.

Additionally, we noted that that the auditing function in Active Directory allows the system to log security, system, and event-related information concerning the success and failure of specified events (e.g. logon and logoff, security policy changes, file access, etc.). Although this function has been activated, there is currently no process in place to review these audit logs.

***Recommendation***

We recommend that effective documentation and mechanisms be put in place to log security activity and identify potential violations. Procedures should also be established to escalate and act upon them in a timely manner to reduce the risk of unauthorized/inappropriate access to the Department's relevant financial reporting applications or data. Evidence of the review (i.e. signoff) should be retained.

***Management Response***

The Information Security Managers will establish, procedures to:

1. Log security activity and identify potential violations in RACF and AD.
2. Escalate and act upon potential violations in a timely manner.
3. Retain evidence of the review and signoff to facilitate the periodic access by Enterprise IT Security Group and Auditors.

## 10. Programmers' Authorization to Migrate Changes to Production

***Observation***

Based on our testwork, we noted that the Department does not restrict or require authorization for programmers to migrate changes to production, and that programmers do indeed have access to migrate code into production. Not restricting developers' ability to migrate changes into application increases the Department's exposure to potential fraudulent and undetectable modification of its systems and data.

***Recommendation***

We recommend that management enable system logging within the key financial applications. All source code migrated to production by a programmer should be logged and periodically reviewed to ensure that all changes made by a programmer/developer were authorized and appropriately approved. This periodic review of migrated code would help mitigate the risk of potential fraudulent and undetectable modifications to the system and data from occurring.

***Management Response***

Current procedures govern the migration of changes for key financial mainframe enterprise applications including APS, EIS, and RCAS. A separation of duties currently exists for mainframe applications. Programmers move changes to turnover libraries using the Please Turnover (PTO) system and document the change in a Technical Change Notice (TCN) and Production Turnover Document (PTD). The Data Centers Production Control group migrates the changes from the staging libraries to production environment. The Instant Change Procedure (ICN) allows programmers to migrate changes to production in the event of an emergency, these changes are reviewed by the Production Control group.

Separation of duties is being developed for distributed applications.

The Senior Systems Analyst is in the process of establishing new change management and release management procedures for both the mainframe and distributed environments using ITIL as a guide. Current procedures will be expanded to include purchased packages like Walker/GL and HRMS as well as distributed systems.

Procedures will be put in place to limit the migration of application changes and have the DBAs migrate code changes into the production environment for the HRMS and Walker G/L systems.

## 11. Informal Process of Walker General Ledger Application Changes/Inappropriate Access for Application Changes

***Observation***

Based on our testwork, we noted the process of applying changes to the application server environment of Walker GL is informal; currently, no formal procedures exist to address the testing of changes and management approval prior to migration into production. Though the lack of oversight over the migration of custom reports into production does not affect the integrity of data within Walker GL, it allows for misrepresentation of GL information on generated reports and potential misstatement.

Additionally, we noted that developers have access to migrate changes into the production environment of the Walker GL application server. Not restricting developers' ability to migrate changes into application increases the Department's exposure to potential fraudulent and undetectable modification of its systems and data.

***Recommendation***

General change control principles suggest that application programmers should not have access to program source or object modules during the approval process. Application programmers should not have update access to programs after they have been approved and before they are moved into production.

To comply with basic general control principles, we recommend the following:

- All changes should be reviewed by a programmer other than the one developing the code to ensure that information will be consistently processed in a controlled environment.
- Changes should be migrated into production by someone other than the developer.
- All approvals (i.e. testing, user acceptance, migration, etc.) should be captured on the Change Request Form.

We recommend that management implement a consistent approach in managing system change requests. Users should convey all system change requests to the system management using some type of formal correspondence, such as a standard change request form, memo, or email. The user request should include, at a minimum, the requestor's name, date of the request, date the change is needed, priority of the request, a thorough description of the change request, and a description of any anticipated effects on other systems or programs. The request should provide evidence that it has been reviewed and authorized by user management. All requests for changes and related information should be maintained by the system maintenance staff as part of the system's permanent documentation.

In addition, we recommend that management enable system logging within the key financial applications. All source codes migrated to production by a programmer should be logged and periodically reviewed to ensure that all changes made by a programmer/developer were authorized and appropriately approved. This periodic review of migrated code would help mitigate the risk of potential fraudulent and undetectable modifications to the system and data from occurring.

***Management Response***

Current procedures govern the migration of changes for key financial mainframe enterprise applications including (APS, EIS, and RCAS). A separation of duties currently exists for mainframe applications. Programmers move changes to turnover libraries using the Please Turnover (PTO) system and document the change in a Technical Change Notice (TCN) and Production Turnover Document (PTD). The Data Centers Production Control group migrates the changes from the staging libraries to production environment. The Instant Change Procedure (ICN) allows programmers to migrate changes to production in the event of an emergency, these changes are reviewed by the Production Control group.

Separation of duties is being developed for distributed applications.

The Senior Systems Analyst will coordinate the establishment of new change management and release management procedures for both the mainframe and distributed environments using ITIL as a guide. Current procedures will be expanded to include purchased packages like Walker/GL and HRMS as well as distributed systems.

In the interim, procedures will be put in place to limit the migration of application changes and have the DBAs migrate code changes into the production environment for the HRMS and Walker G/L systems.

**12. Retention of Production Control Turnover Sheets**

***Observation***

Based on our testwork, we noted that the 'Production Control Turnover Sheets', used for monitoring and logging of mainframe system jobs and data processing, are only maintained for a period of 4 months.

***Recommendation***

We recommend that management implement a policy regarding the retention of the 'Production Control Turnover Sheets'. Evidence of the monitoring and logging of the mainframe system jobs should be retained for a period of twelve (12) months. This document retention will facilitate auditability of the control and help substantiate the operating effectiveness of this control for the entire fiscal year audit period.

***Management Response***

We agreed with the recommendation. As of April 9, 2008, the retention of the Daily Turnover Log has been extended from four (4) month to twelve (12) Months.

**13. Ineffective Disaster and Recovery Testing Process**

***Observation***

Based on our testwork, we noted that the 'Disaster Recovery Test Results Summary Narrative', for both August 2006 and November 2006, did not contain actual results of the disaster recovery test but only a high level overview of the test performed. In addition, the 'Rescue Test Checklists' had not been appropriately completed as several tasks remained unchecked. We noted that while policies, procedures, running narrative and task lists for disaster, and recovery testing are in place, the summary and checklist had insufficient documentation to provide reasonable assurance that the semiannual disaster and recovery testing were operating effectively.

***Recommendation***

We recommend that management recommunicate the policy and procedures regarding the appropriate documenting of the 'Disaster Recovery Test Results'. Within the results documentation, actual results, outcomes, issues, and concerns should be well documented for referencing during future disaster recovery testing. Management should ensure the appropriate completion of the

'Disaster Recovery Test Results Summary' and the 'Rescue Test Checklists' by personnel involved with the disaster recovery test.

***Management Response***

The Information Security Manager will review and revise the current Restoration Testing policies (in collaboration with Enterprise IT Security Section) and procedures to include both mainframe and distributed systems. Testing shall include of a sample of data from media stored off-site. The revised policies and procedures will be redistributed.

In addition, the current templates are being revised so that actual results, outcomes, issues, concerns are documented for reference during future disaster recovery tests.

The Information Security Manager will review the 'Disaster Recovery Test Results Summary' and the 'Rescue Test Checklists' after each disaster recovery test to ensure the appropriate completion of documentation.

## 14. Untimely Resolution of Reported Application Problems

***Observation***

Based on our test work, we noted out of the fifteen (15) incidents, thirteen (13) incidents were resolved outside of their allotted timeframe for the various priorities of urgent, high, and medium.

***Recommendation***

We recommend that management recommunicate the formal policies and procedures over incident management and the resolution of identified incidents to appropriate personnel. Management has a formal process in place to ensure proper information and details of an incident are evidenced and captured. However, the guidance over the timeliness of the resolution should be formalized and reviewed by management to ensure compliance. Similar to a change management methodology, appropriate approvals, testing, and migration information should be formally captured and documented for all steps taken to resolve the incident/failure.

***Management Response***

The Information Systems Manager will review and re-communicate the current policy and procedures over incident management and resolution of identified incidents, which will include capturing and documenting steps taken to resolve the incident/failure to appropriate personnel.

The Information Systems Manager will develop a policy (in collaboration with Enterprise IT Security Section) and procedures to ensure proper information and details of an incident are evidenced and captured and that the timeliness of the resolution be formalized and reviewed by management to ensure compliance.

## 15. Inappropriate Query Tools for Materials Controls System (MCS)

***Observation***

Based on our testwork, we were unable to verify the completeness of 'Material Control System Report – Total Receipts and Issues by Document Code By Store Number' report (SG0750P1) as the

format of the underline data could not be easily interpreted for analysis. In addition, we noted that MCS is a legacy system utilizing the IMS database. Currently, the Department does not have appropriate tools to query the database to provide the required summation of transactions.

***Recommendation***

We recommend that management performs an annual audit of certificated 'Material Control System Report – Total Receipts and Issues by Document Code by Store Number' report (SG0750P1) to determine that all materials are accounted for accurately and completely.

***Management Response***

The material management group performs a monthly audit, which is reviewed periodically by management. The most recent management review occurred in June 21, 2007.

## 16. Inappropriate Access within the HRMS Application

***Observation***

Based on our testwork, we noted seventeen (17) active user accounts with access to change employee salary rates in HRMS. Five (5) out of these 17 users have inappropriate access. The PeopleSoft security administrator has access to update salary rates, which is a segregation of duties conflict. This creates a segregation of duties conflict. Four (4) inappropriate users are from the Information Technology Services (ITS) department and have excessive ITS access to the production environment. Per inspection, we noted that two were identified as Programmer/Analysts; two were identified as Database Architects.

***Recommendation***

We recommend that management perform an assessment over users with access to change employee salary rates within HRMS. Access should be determined as appropriate if the user requires this specific access to perform their daily job responsibilities. If inappropriate access is identified, they should be terminated immediately. Careful considerations towards maintaining appropriate segregation of duties must be taken. Access to change employee salary rates should be appropriately restricted to approved individuals.

On an ongoing basis, we recommend management perform a periodic review of users with access to key financial applications to ensure that access is appropriately restricted and high risk access is only granted to authorized personnel with the daily job responsibilities, which require this access. This review will help ensure that an employees' access to the key financial applications is in line with their job responsibilities as well as maintain proper segregation of duties within key financial processes.

***Management Response***

The Information Security Manager is in the process of developing a policy (in collaboration with Enterprise IT Security Section) and procedures to perform Periodic Review of User Access Rights.

For the HRMS system, a formal request form is currently in place as part of the ITSR system. The ITSR system requires appropriate approvals prior to access being granted.

The Information Security Manager will collaborate with business users to develop a role based security access matrix, which will address segregation of duty conflicts. This matrix will be used to develop and review and revise if necessary security groups to protect sensitive transactions.

The Information Security Manager will develop a policy (in collaboration with Enterprise IT Security Section) and procedure requiring a formal review by management of HRMS access rights.

A more complete Identity Management solution providing access management and provisioning solution is currently being investigated. The projected schedule for the project is as follows:

| | |
|---|---|
| Project Start | May 2008 |
| Web Access | July 2008 |
| Central repository | Nov 2008 |
| Initial Provisioning | Feb 2009 |

**17. Inappropriate Access to Integrated Purchasing and Receiving System (IPRS)**

***Observation***

Based on our testwork, we noted twenty-nine (29) of one hundred and fifty-nine (159) users have inappropriate access to input the receipt of goods into IPRS at the various stores/warehouse locations.

***Recommendation***

We recommend that management perform an assessment over users with access to input the receipt of goods into IPRS at the various store/warehouse locations. Access should be determined as appropriate if the user requires this specific access to perform their daily job responsibilities. If inappropriate access is identified, these access should be removed immediately. Management should carefully identify and review all users that require access to input the receipt of goods and ensure that access is appropriately restricted to these approved individuals.

On an ongoing basis, we recommend management perform a periodic review of users with access to key financial applications to ensure that access is appropriately restricted and high risk access is only granted to authorized personnel with the daily job responsibilities, which require this access. This review will help ensure that an employees' access to the key financial applications is in line with their job responsibilities as well as maintain proper segregation of duties within key financial processes.

***Management Response***

The Information Systems Manager will develop a policy (in collaboration with Enterprise IT Security Section) and procedures to perform Periodic Review of User Access Rights. There was a review of access rights mid-year 2007. For IPRS, a formal request form is currently in place as part of the ITSR system. The ITSR system requires appropriate approvals prior to granting of access.

The Information Systems Manager will collaborate with business users to develop a role based security access matrix, which will address segregation of duty conflicts. This matrix will be used to develop and review and revise, if necessary security groups to protect sensitive transactions.

A more complete Identity Management solution providing access management and provisioning solution is currently being investigated. The projected schedule for the project is as follows:

| | |
|---|---|
| Project Start | May 2008 |
| Web Access | July 2008 |
| Central repository | Nov 2008 |
| Initial Provisioning | Feb 2009 |